03 014
RPS

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　２月　６日
出願番号 Application Number:	特願２００３－０２９８１３
[ST. 10/C]:	[ＪＰ２００３－０２９８１３]
出願人 Applicant(s):	インターナショナル・ビジネス・マシーンズ・コーポレーション

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０５７８００

【書類名】　特許願

【整理番号】　JP09030014

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/32

G06F 15/00

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　緒方　栄次

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100108501

【弁理士】

【氏名又は名称】　上野　剛史

【復代理人】

【識別番号】　100085408

【弁理士】

【氏名又は名称】　山崎　隆

【手数料の表示】

【予納台帳番号】　117560

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0207860

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、情報処理装置用制御方法、及び情報処理装置用制御プログラム

【特許請求の範囲】

【請求項１】　セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェア、

ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればＯＳ起動を許容するＯＳ起動許容手段、

所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段、

前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第１のシステム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容手段が作動する第１の形式のＯＳ起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第２のシステム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容手段が作動しない機能制限された第２の形式のＯＳ起動とのいずれかを選択して実施するＯＳ起動形式選択手段、

第２のシステム状態の期間に生成され第１の形式のＯＳ起動における前記ＯＳ起動許容手段の作動を無効にする無効化手段、及び

前記ＯＳ起動許容手段が前記無効化手段により作動を無効化された第１の形式のＯＳ起動が少なくとも１回、実施された後、前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除する無効解除手段、

を有していることを特徴とする情報処理装置。

【請求項２】　ユーザ認証用の入力データは、第１の形式のＯＳ起動の際にユーザがキー入力するデータであることを特徴とする請求項１記載の情報処理装置。

【請求項３】　前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のもの

として生成されたものであり、補助記憶装置に保存されているものであることを特徴とする請求項１記載の情報処理装置。

【請求項４】　第１及び第２の形式のＯＳ起動は、同一の補助記憶装置内に保存されている同一のＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、ＯＳを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第１の形式のＯＳ起動を、また、”有り”のときは第２の形式のＯＳ起動を、それぞれ選択して実施するものであることを特徴とする請求項１記載の情報処理装置。

【請求項５】　第１及び第２の形式のＯＳ起動は、それぞれ別の補助記憶装置内に保存されているＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、前記第２のＯＳを保存する補助記憶装置から前記第２のＯＳを読み取り可能であるときは、第１の形式のＯＳ起動より第２の形式のＯＳ起動を優先して、選択し、実施するものであることを特徴とする請求項１記載の情報処理装置。

【請求項６】　前記無効解除手段が前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除した後に、前記無効解除手段を消去する消去手段を有していることを特徴とする請求項１記載の情報処理装置。

【請求項７】　前記消去手段は前記無効解除手段により生成されるものであることを特徴とする請求項６記載の情報処理装置。

【請求項８】　セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェア、

ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればＯＳ起動を許容するＯＳ起動許容手段、

所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段、

前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第１のシステム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容手段が作動する第１の形式のＯＳ起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第２のシステ

ム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容ステップが作動しない機能制限された第２の形式のＯＳ起動とのいずれかを選択して実施するＯＳ起動形式選択手段、
を有する情報処理装置の制御方法であって、
次の各ステップをコンピュータに実行させる情報処理装置の制御方法であって、
無効化手段が、それが生成された以降の第１の形式のＯＳ起動における前記ＯＳ起動許容手段の作動を無効にする無効化ステップ、及び
前記ＯＳ起動許容手段が前記無効化手段により作動を無効化された第１の形式のＯＳ起動が少なくとも１回、実施された後、無効解除手段が、前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除する無効解除ステップ、
を有していることを特徴とする情報処理装置用制御方法。

【請求項９】　ユーザ認証用の入力データは、第１の形式のＯＳ起動の際にユーザがキー入力するデータであることを特徴とする請求項８記載の情報処理装置用制御方法。

【請求項１０】　前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置に保存されているものであることを特徴とする請求項８記載の情報処理装置用制御方法。

【請求項１１】　第１及び第２の形式のＯＳ起動は、同一の補助記憶装置内に保存されている同一のＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、ＯＳを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第１の形式のＯＳ起動を、また、”有り”のときは第２の形式のＯＳ起動を、それぞれ選択して実施するものであることを特徴とする請求項８記載の情報処理装置用制御方法。

【請求項１２】　第１及び第２の形式のＯＳ起動は、それぞれ別の補助記憶装置内に保存されているＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、前記第２のＯＳを保存する補助記憶装置から前記第２のＯＳを読み取り可能であるときは、第１の形式のＯＳ起動より第２の形式のＯＳ起動を優先して、選択

し、実施するものであることを特徴とする請求項８記載の情報処理装置用制御方法。

【請求項１３】　前記無効解除手段が前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除した後に、消去手段が前記無効解除手段を消去する消去ステップ、

を有していることを特徴とする請求項８記載の情報処理装置用制御方法。

【請求項１４】　前記無効解除手段が前記消去手段を生成するステップ、

を有していることを特徴とする請求項１３記載の情報処理装置用制御方法。

【請求項１５】　請求項８～１３のいずれかの情報処理装置用制御方法における各ステップをコンピュータに実行させることを特徴とする情報処理装置用制御プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、パーソナル・コンピュータ等の情報処理装置、情報処理装置用制御方法及び情報処理装置用制御プログラムに係り、詳しくはセキュリティ・ハードウェアを装備しシステム・ログオン時にセキュリティ・ハードウェア内のセキュリティ・キー情報に基づいてユーザ認証を行うようになっている情報処理装置、情報処理装置用制御方法、及び情報処理装置用制御プログラムに関するものである。

【０００２】

【従来の技術】

ＴＣＰＡ（Trusted Computing Platform Alliance：”http://www.trustedcomputing.org/tcpaasp4/index.asp”）の規格に準拠したセキュリティ・チップを装備するＰＣ（パーソナル・コンピュータ）では、セキュリティ・チップにおける所定の暗号プログラムやセキュリティ・キー情報を使用して、種々のセキュリティ処理、例えば、ＯＳ（Operating System：オペレーティング・システム）起動を許可すべきか否かのユーザ認証、ＯＳとの連携によるファイルやフォルダの暗号化及び復号、デジタル証明書の保管、並びに各種アプリケーションにおけるユ

ーザ認証の統合化等を実施している。

【０００３】

一方、特許文献１は、端末に接続された認証装置を介してＩＣカード等のセキュリティ・ハードウェア内のセキュリティ・キー情報を読み取り、セキュリティ・キー情報に基づきセキュリティ・ハードウェアの所有者が正当な所有者であるか否かを判断し、判断結果が正であるときのみ、端末からホストへのログインを許容している。

【０００４】

【特許文献１】

特開２００１－９９４６６号

【０００５】

【発明が解決しようとする課題】

ＰＣにおいて通常のハードウェアの故障に係る修理では、故障したハードウェアを新規なものと交換すれば足りる。これに対して、ＴＣＰＡ準拠のセキュリティ・チップの交換を含む修理を行う場合には、交換後の新規なセキュリティ・チップには、交換前のセキュリティ・チップ内に保存していたセキュリティ・キー情報が存在しないので、セキュリティ・チップの交換後にＰＣに電源投入しても、ＯＳ起動（以下、適宜、「システム・ログオン」と言う。）ができず、すなわち、ＰＣの使用が困難になる。すなわち、セキュリティ・チップ内のセキュリティ・キー情報は、セキュリティ・チップ内の所定のプログラムにより暗号化されて、セキュリティ・チップ内に保存されており、セキュリティ・キー情報に基づくシステム・ログオン用ユーザ認証を行うためには、セキュリティ・チップ内のセキュリティ・キー情報をセキュリティ・チップ内のプログラムにより復号する必要があり、セキュリティ・チップ内にセキュリティ・キー情報が無いと、この復号は困難になるので、ユーザ認証が実施できず、システム・ログオンが困難になる。これを克服するには、ＰＣへＯＳを再インストールしてから、セキュリティ・キー情報を新規に設定し直す必要があり、労力と時間が膨大になる。また、交換前のセキュリティ・チップ内のセキュリティ・キー情報に基づいて暗号化されてハード・ディスクに保存されているフォルダやファイルは、交換前のセキュ

リティ・チップのセキュリティ・キー情報に基づいて暗号化されているので、新規のセキュリティ・チップについて別途、新規のセキュリティ・キー情報を登録しても、復号は困難である。ＴＣＰＡ準拠のセキュリティ・チップは、通常、マザーボードに組み付けられており、典型的な修理では、マザーボードのどれかの素子が故障したときには、マザーボード全体が交換されるので、セキュリティ・チップ自体は壊れていなくても、セキュリティ・チップが交換されるケースは多い。

【０００６】

特許文献１は、正当なセキュリティ・ハードウェアに基づいて認証を受けて、一度、端末からホストへログインした後、セキュリティ・ハードウェアが悪意に正当なものから不正なものへ交換されて、セッションが継続する事態に対処するための方策は開示しているものの、正当なユーザが、セキュリティ・ハードウェアを交換したときに、交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を使用じなければ、システム・ログオンして、交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を新規なセキュリティ・ハードウェアに復元できない場合に、セキュリティ・キー情報を交換後のセキュリティ・ハードウェアに復元する有効な方策についてはなんら開示していない。

【０００７】

本発明の目的は、システム・ログオンするためには交換前のセキュリティ・ハードウェアのセキュリティ・キー情報が必要であり、また、交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を交換後のセキュリティ・バードウェアに復元するためには、システム・ログオンする必要のある情報処理装置において、交換後の新規のセキュリティ・ハードウェアに交換前のセキュリティ・ハードウェアのセキュリティ・キー情報を復元できる情報処理装置、情報処理装置用制御方法、及び情報処理装置用制御プログラムを提供することである。

【０００８】

【課題を解決するための手段】

本発明の情報処理装置は次のものを有している。

・セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェア

・ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればＯＳ起動を許容するＯＳ起動許容手段

・所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段

・前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第１のシステム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容手段が作動する第１の形式のＯＳ起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第２のシステム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容手段が作動しない機能制限された第２の形式のＯＳ起動とのいずれかを選択して実施するＯＳ起動形式選択手段

・第２のシステム状態の期間に生成され第１の形式のＯＳ起動における前記ＯＳ起動許容手段の作動を無効にする無効化手段

・前記ＯＳ起動許容手段が前記無効化手段により作動を無効化された第１の形式のＯＳ起動が少なくとも１回、実施された後、前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除する無効解除手段

【０００９】

本発明によれば、第１の形式のＯＳ起動とは別の形式としての第２の形式のＯＳ起動を利用する。第１の形式のＯＳ起動とは、例えば、標準のＯＳ起動であり、機能制限の無いシステム状態に情報処理装置を立ち上げるときのＯＳ起動である。これに対して、第２の形式のＯＳ起動とは、例えば、非常時又は緊急避難時のＯＳ起動であり、最小限の機能で情報処理装置を作動させるシステム状態を確保するときのＯＳ起動である。例えばＯＳとしてＷｉｎｄｏｗｓ　ＮＴ，Ｗｉｎｄｏｗｓ　２０００，Ｗｉｎｄｏｗｓ　ＸＰ（いずれも登録商標）を装備するＰＣ（パーソナル・コンピュータ）では、標準のＯＳ起動は、ユーザがＰＣの電源投入するのみで、他の特別のユーザ操作を要求されずに、実行されるものである。これに対して、第２の形式のＯＳ起動としてのセーフ・モード用ＯＳ起動は、ユーザが、ＰＣの電源投入後、例えばキー・ボードのＦ８キーを押し続けるとい

う所定のユーザ操作があったときに実行される。第２の形式のＯＳ起動では、機能制限のために、セキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証をスキップして、情報処理装置を第２のシステム状態にすることができる。第２のシステム状態期間では、機能制限のために、セキュリティ・ハードウェアのセキュリティ・キー情報の復元処理は困難であるが、以降の第１の形式のＯＳ起動におけるセキュリティ・ハードウェアのセキュリティ・キー情報に係る認証処理の無効化等の設定は可能である。なぜなら、これらの設定は、低レベルの機能であり、第２のシステム状態では、所定レベル以下の機能の実行は可能であるからである。第２のシステム状態の例としてのセーフ･モードでは、ＦＤ（フロッピ・ディスク）からハード・ディスクへのプログラム･ファイルのコピーや、次回以降の標準モードの起動における設定は可能である。こうして、第２のシステム状態における所定のプログラムの実行により、無効化手段を含むコンピュータ・ソフトウェアが生成される。無効化手段は、それが生成された以降の第１の形式のＯＳ起動の際には、ＯＳ起動許容手段の作動を無効化し、これにより、ＯＳ起動許容手段によるユーザ認証を経ずに、情報処理装置を第１のシステム状態にすることができる。こうして実現された第１のシステム状態において、セキュリティ・ハードウェアにおけるセキュリティ・キー情報が復元される。無効解除手段は、次回からの第１の形式のＯＳ起動では、ＯＳ起動許容手段によるセキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証処理を有効化するように、作動する。結果、新規のセキュリティ・ハードウェアに交換された情報処理装置において、交換前のセキュリティ・ハードウェアを装備していた情報処理装置のときと同一のセキュリティ・キー情報に基づくシステム・ログオン及びその他の処理が実施される。

【００１０】

本発明の情報処理装置は、上述の情報処理装置に対して、次の（ａ１）～（ａ６）の１個又は複数個を任意の組み合わせで付加したものを含む。

（ａ１）ユーザ認証用の入力データは、第１の形式のＯＳ起動の際にユーザがキー入力するデータであること。

（ａ２）前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・

キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置に保存されているものであること。

（ａ３）第１及び第２の形式のＯＳ起動は、同一の補助記憶装置内に保存されている同一のＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、ＯＳを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第１の形式のＯＳ起動を、また、”有り”のときは第２の形式のＯＳ起動を、それぞれ選択して実施するものであること。

（ａ４）第１及び第２の形式のＯＳ起動は、それぞれ別の補助記憶装置内に保存されているＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、前記第２のＯＳを保存する補助記憶装置から前記第２のＯＳを読み取り可能であるときは、第１の形式のＯＳ起動より第２の形式のＯＳ起動を優先して、選択し、実施するものであること。

（ａ５）前記無効解除手段が前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除した後に、前記無効解除手段を消去する消去手段をさらに有していること。

（ａ６）上記（ａ５）において、前記消去手段は前記無効解除手段により生成されるものであること。

【００１１】

本発明の情報処理装置用制御方法が適用される情報処理装置は、セキュリティ・キー情報を読書き自在に格納するセキュリティ・ハードウェアと、ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、前記セキュリティ・ハードウェアから読み出した前記セキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればＯＳ起動を許容するＯＳ起動許容手段と、所定の復元用データに基づいてセキュリティ・ハードウェアにセキュリティ・キー情報を復元するセキュリティ・キー情報復元手段と、前記セキュリティ・キー情報復元手段が作動可能となるシステム状態（以下、「第１のシステム状態」と言う。）を生成するＯＳ起動であってかつ前記ＯＳ起動許容手段が作動する第１の形式のＯＳ起動と、前記セキュリティ・キー情報復元手段が作動不可能である機能制限されたシステム状態（以下、「第２のシステム状態」と言う。）を生成するＯＳ起動で

あってかつ前記ＯＳ起動許容ステップが作動しない機能制限された第２の形式のＯＳ起動とのいずれかを選択して実施するＯＳ起動形式選択手段と、を有する。そして、本発明の情報処理装置用制御方法は次のステップを有している。

・無効化手段が、それが生成された以降の第１の形式のＯＳ起動における前記ＯＳ起動許容手段の作動を無効にするように、第２のシステム状態の期間に前記無効化手段を生成する無効化手段生成ステップ

・前記ＯＳ起動許容手段が前記無効化手段により作動を無効化された第１の形式のＯＳ起動が少なくとも１回、実施された後、無効解除手段が、前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除するように、前記無効解除手段を生成する無効解除手段生成ステップ

【００１２】

本発明の情報処理装置用制御方法は、上述の情報処理装置用制御方法に対して、次の（ｂ１）～（ｂ６）の１個を又は複数個を任意の組み合わせで付加したものを含む。

【００１３】

（ｂ１）ユーザ認証用の入力データは、第１の形式のＯＳ起動の際にユーザがキー入力するデータであること。

（ｂ２）前記復元用データは、セキュリティ・ハードウェア内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置に保存されているものであること。

（ｂ３）第１及び第２の形式のＯＳ起動は、同一の補助記憶装置内に保存されている同一のＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、ＯＳを起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第１の形式のＯＳ起動を、また、”有り”のときは第２の形式のＯＳ起動を、それぞれ選択して実施するものであること。

（ｂ４）第１及び第２の形式のＯＳ起動は、それぞれ別の補助記憶装置内に保存されているＯＳに基づく起動であり、前記ＯＳ起動形式選択手段は、前記第２のＯＳを保存する補助記憶装置から前記第２のＯＳを読み取り可能であるときは、第１の形式のＯＳ起動より第２の形式のＯＳ起動を優先して、選択し、実施する

ものであること。

（ｂ５）前記無効解除手段が前記無効化手段による前記ＯＳ起動許容手段の作動の無効を解除した後に、消去手段が前記無効解除手段を消去する消去ステップを有していること。

を有していることを特徴とする請求項８記載の情報処理装置。

（ｂ６）上記（ｂ５）のステップに加えて、前記無効解除手段が前記消去手段を生成するステップを有していること。

【００１４】

本発明の情報処理装置用制御プログラムは、本発明の情報処理装置用制御方法における各ステップをコンピュータに実行させる。

【００１５】

【発明の実施の形態】

以降、本発明を実施の形態について具体的に説明する。なお、本発明は実施の形態及び実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。図面全般にわたる構成を先に説明してから、情報処理装置１０の修理者によるセキュリティ・キー情報の復元作業の手順に則して、情報処理装置１０の作用について説明する。

【００１６】

図１は情報処理装置１０のブロック図である。図１において、無効化手段１５のブロックは斜線を施されているが、これは、無効化手段１５が第２のシステム状態において生成されることを意味する。なお、無効解除手段１６は、無効化手段１５によるＯＳ起動許容手段１２の作動無効後に、該無効を解除するように設定してあれば、第１のシステム状態ではなく、無効化手段１５と同様に、第２のシステム状態において生成されてもよい。無効解除手段１６は、例えば、無効化手段１５がＯＳ起動許容手段１２の作動を無効にした第１の形式のＯＳ起動による第１のシステム状態において生成される。セキュリティ・ハードウェア１１は、セキュリティ・キー情報を読書き自在に格納（ストア）する。ＯＳ起動許容手段１２は、ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、セキュリティ・ハードウェア１１から読み出したセキュリティ・キー情報に基づい

て判断し、該判断結果が”正”であればＯＳ起動を許容する。セキュリティ・キー情報復元手段１３は、所定の復元用データに基づいてセキュリティ・ハードウェア１１にセキュリティ・キー情報を復元する。ＯＳ起動形式選択手段１４は、セキュリティ・キー情報復元手段１３が作動可能となるシステム状態（以下、「第１のシステム状態」と言う。）を生成するＯＳ起動であってかつＯＳ起動許容手段１２が作動する第１の形式のＯＳ起動と、セキュリティ・キー情報復元手段１３が作動不可能である機能制限されたシステム状態（以下、「第２のシステム状態」と言う。）を生成するＯＳ起動であってかつＯＳ起動許容手段１２が作動しない機能制限された第２の形式のＯＳ起動とのいずれかを選択して実施する。無効化手段１５は、第２のシステム状態の期間に生成され、第１の形式のＯＳ起動におけるＯＳ起動許容手段１２の作動を無効にする。注釈すると、無効化手段１５は、第１の形式のＯＳ起動におけるＯＳ起動許容手段１２の作動を無効にする処理を実施するが、該処理は、当然に、それが生成されてからのことであり、生成前に該処理の実施氏は困難である。ＯＳ起動許容手段１２が無効化手段１５により作動を無効化された第１の形式のＯＳ起動が少なくとも１回、実施された後、無効化手段１５によるＯＳ起動許容手段１２の作動の無効を解除する。

【００１７】

典型的には、ＯＳ起動許容手段１２が無効化手段１５により作動を無効化された第１の形式のＯＳ起動が１回だけ、実施されしだい、無効化手段１５によるＯＳ起動許容手段１２の作動の無効を解除する。しかし、無効解除の時期は、第１の形式のＯＳ起動が複数の所定回数、実施された後であったり、１回目の実施時刻から所定時間経過後の最初の第１の形式のＯＳ起動の時又は第１のシステム状態の期間であってもよい。

【００１８】

図２は携帯型ＰＣ（パーソナル・コンピュータ）１８及びデスク・トップ型ＰＣ１９を示す。情報処理装置１０は、例えば、携帯型ＰＣ３８及びデスク・トップ型ＰＣ３９であり、さらに、その他のＰＣ、ＰＤＡ（Personal Digital Assistant）、携帯電話、家電、及びゲーム機であってもよい。

【００１９】

セキュリティ・ハードウェアは、マザーボード上のセキュリティ・チップに制限されず、ＩＣカードや、さらに、ＰＣのＵＳＢ（Universal Serial Bus）等の周辺機器接続用コネクタに、ケーブルを介さずに直接、差し込まれる携帯型メモリ・デバイス等の他のセキュリティ・ハードウェアであってもよい。セキュリティ・チップは典型的にはＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory。電気的に消去（書き換え）できるＲＯＭ）である。ＯＳは、情報処理装置がＰＣである場合は、例えば、Ｗｉｎｄｏｗｓ　ＮＴ，Ｗｉｎｄｏｗｓ　２０００，Ｗｉｎｄｏｗｓ　ＸＰ、ＤＯＳ（いずれも登録商標）のほか、Ｌｉｎｕｘ、Ｍａｃ　ＯＳ（登録商標）、及びＴＲＯＮ用ＯＳ等、他のＯＳであってもよい。ＯＳがＷｉｎｄｏｗｓである場合、第１及び第２のシステム状態はそれぞれ標準モード及びセーフ・モードに対応する。

【００２０】

ユーザ認証用の入力データは、例えば第１の形式のＯＳ起動の際にユーザがキー入力するデータである。図３はセキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証用の窓を例示したものである。図３の窓は、情報処理装置１０としてのＰＣでは、第１の形式のＯＳ起動の際にＰＣのディプレイに表示される。ユーザは、図３の窓に対して、ユーザ名の欄及びパスフレーズの欄に、自己に係るユーザ名及びパスフレーズ（例：”本日は晴天なり”）を、キーボードを使って入力する。その次に、”ＯＫ”ボタンをクリックすると、ユーザ名及びパスフレーズがＣＰＵに取り込まれ、セキュリティ・ハードウェア１１内のセキュリティ・キー情報に係るデータと照合され、ユーザが正当であると認証されれば、第１の形式のＯＳ起動が実行される。ＯＳ起動の際にユーザ認証用の入力データは、ユーザがキーボードを介して入力するパスワードやパスフレーズに限定されず、ユーザから検出したユーザの指紋や虹彩に係るデータであってもよい。

【００２１】

図４はＯＳに基づくユーザ認証用窓の例示である。システム・ログオン時におけるＯＳに基づくユーザ認証は、図３に係るセキュリティ・ハードウェア１１のセキュリティ・キー情報に基づくユーザ認証は、図４に係るシステム・ログオン

時におけるＯＳに基づくユーザ認証とは別個のものである。ユーザは、図４のユーザ認証用窓に対してユーザ名及びパスワードを各欄に入力する。ＰＣのセキュリティのためにセキュリティ・ハードウェア１１としてのセキュリティ・チップをＰＣにおいて利用するソフトウェア（以下、該ソフトウェアを「ＣＳＳ（Ｃｌｉｅｎｔ　Ｓｅｃｕｒｉｔｙ　Ｓｏｆｔｗａｒｅ）」と呼ぶことにする。）は、セキュリティ・チップを装備したＰＣを購入したユーザがインターネットの所定のサイトより適宜、ＰＣへダウンロードするようになっており、該ＣＳＳでは、ＯＳや各アプリケーションでの認証を、システム・ログオン時のセキュリティ・チップのセキュリティ・キー情報に基づく認証に統合できるようになっている。すなわち、ＣＳＳでは、設定により、ＰＣのユーザは、システム・ログオン時に、セキュリティ・チップのセキュリティ・キー情報に基づく認証を１回、受けさえすれば、そのシステム・ログオン中、繰返して他のユーザ認証を受けなくて済むようになっている。

【００２２】

復元用データは、例えば、セキュリティ・ハードウェア１１内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、ハード・ディスクのような補助記憶装置に保存されているものである。図５はセキュリティ・ハードウェア１１におけるセキュリティ・キー情報を復元する際の作業窓を例示する。ＣＳＳは、システム・ログオンの許可等のユーザ認証、ＯＳとの連携によるファイルやフォルダの暗号化及び復号、デジタル証明書の保管、並びに各種アプリケーションにおけるユーザ認証の統合化の他に、セキュリティ・チップへのセキュリティ・キー情報の新規登録、セキュリティ・チップへ登録済みのセキュリティ・キー情報の削除、及びセキュリティ・キー情報の復元の機能を装備している。ＣＳＳでは、セキュリティ・キー情報を作成する際、セキュリティ・キー情報の復元を実現するための復元実現用ファイルが該セキュリティ・キー情報の対として生成される。このような復元実現用ファイルは、好ましくは、ＦＤにアーカイブ・ファイルによりストアしておき、情報処理装置１０のユーザは、該ＦＤを適切な場所に保管しておく。しかし、復元実現用アーカイブ・ファイルはハード・ディスクに保存してもよい。復元実現

用アーカイブ・ファイルを所定のＦＤに保管しておくときは、情報処理装置１０の修理者は、ユーザより該ＦＤを預かるか、ユーザよりメールで送付して貰うか、予めハード・ディスクの所定のフォルダにストアしておいて貰うか等する。修理者は、図５のセキュリティ・キー情報復元用窓において、復元実現用アーカイブ・ファイル、公開鍵ファイル、及び秘密鍵ファイルをそれぞれの入力欄にパスと共に入力する。この入力は、ユーザが直接書き込むことに代えて、”参照”ボタンをクリックして、所定のドライブの所定のフォルダにアクセスして、該当のファイルを選択することにより、実施可能となっている。３個の入力欄に該当のファイルの入力が終わったら、修理者は、”ＯＫ”ボタンをクリックする。こうして、３個の入力欄に入力されたファイルの対応が取れていることが復元実現用アーカイブ・ファイルにより検証されると、セキュリティ・チップには、セキュリティ・キー情報が復元される。なお、ＣＳＳでは、復元実現用ファイルとしてのアーカイブ・ファイル、公開鍵及び秘密鍵の３個の要素からパスフレーズを知ることは可能であるが、アーカイブ・ファイルのみからパスフレーズを知ることは困難になっている。したがって、アーカイブ・ファイルをストアしたＦＤを盗み出されても、盗用者がパスフレーズを知ることはできない。

【００２３】

図６は所定態様のＯＳ起動形式選択手段１４を装備する情報処理装置１０のブロック図である。第１及び第２の形式のＯＳ起動は、同一の補助記憶装置２１（典型的にはハード・ディスク）内に保存されている同一のＯＳ２２に基づく起動である。図６のＯＳ起動形式選択手段１４は、第１及び第２の形式のＯＳ起動の実施手段２３，２４、所定ユーザ操作の検出手段２５、及び切替手段２６、を有している。所定ユーザ操作の検出手段２５は、ＯＳ２２を起動しようとするときに、所定ユーザ操作の有無を検出する。切替手段２６は、該所定ユーザ操作が”無し”であるときは第１の形式のＯＳ起動の実施手段２３を作動させ、また、”有り”であるときは第２の形式のＯＳ起動の実施手段２４を作動させる。

【００２４】

図７は別の所定態様のＯＳ起動形式選択手段１４を装備する情報処理装置１０のブロック図である。第１及び第２の形式のＯＳ起動は、それぞれ別の補助記憶

装置２１，３１内に保存されているＯＳ２２，３２に基づく起動である。補助記憶装置２１，３１は例えばそれぞれハード・ディスク及びＦＤ（フロッピィ・ディスク）である。典型的には、補助記憶装置２１は常設補助記憶装置であり、補助記憶装置３１は交換可能なメディアである。図７のＯＳ起動形式選択手段１４は、第１及び第２の形式のＯＳ起動の実施手段２３，２４、メディア検出手段３４、及び切替手段２６、を有している。メディア検出手段３４は、ＯＳ３２が保存されている補助記憶装置３１からＯＳ３２を読み取り可能であるか否かを検出する。情報処理装置１０は、ＯＳをもつ交換可能メディアがそのメディア用ドライブに存在すれば、ＯＳをもつ常備メディアより優先して、交換可能メディアからＯＳを読み取る方式を採用するので、切替手段２６は、第２の形式のＯＳ起動３２を保存する補助記憶装置３１から第２のＯＳ３２を読み取り可能であるときは、第２の形式のＯＳ起動の実施手段２４を作動させ、また、不可能であるときは、第１の形式のＯＳ起動の実施手段２３を作動させる。

【００２５】

図８は消去手段３７が付加された情報処理装置１０のブロック図である。消去手段３７は、無効解除手段１６が無効化手段１５によるＯＳ起動許容手段１２の作動の無効を解除した後に、無効解除手段１６を消去する。消去手段３７は例えば前記無効解除手段１６により生成されるものである。無効化手段１５及び無効解除手段１６はソフトウェアの機能として実現されるが、該ソフトウェアを所有するものは修理者等の特定の者に限定されることが管理上、望ましい。この場合、修理者は、作業実行後は情報処理装置１０から分離できるＦＤ等の交換可能なメディアから該ソフトウェアを立ち上げ、情報処理装置１０に常備のハード・ディスクには、作業終了後に該ソフトウェアの主要部としての無効化手段１５及び無効解除手段１６が残らないようにする必要がある。無効化手段の１５の機能、すなわち次回以降の第１の形式のＯＳ起動においてＯＳ起動許容手段１２の作動を無効にする設定は、第２のシステム状態において交換可能メディアから実行して、ハード・ディスク内に該ソフトをストアすることを回避できるが、無効解除手段１６を構成するソフトウェア部分は、第２のシステム状態では実行できず、ハード・ディスクにコピーして、実行する必要が生じることがある。しかし、無

効解除手段１６がその機能を実行した直後の期間、例えば次の第１のシステム状態の期間において、プログラム・ファイル削除プログラムのような消去手段３７が無効解除手段１６を消去するようにすれば、無効解除手段１６を構成するソフトウェア部分はハード・ディスクに残ったまま、修理者からユーザに情報処理装置１０が返却されることが防止される。

【００２６】

修理者が情報処理装置１０におけるセキュリティ・ハードウェア１１を交換した修理作業を行ったときに、修理者がセキュリティ・ハードウェア１１にセキュリティ・キー情報を復元する処理手順（Ｒ１）～（Ｒ６）を説明しつつ、情報処理装置１０の作用を説明する。ＯＳがＷｉｎｄｏｗｓである場合、第１及び第２の形式のＯＳ起動はそれぞれ例えば標準モード及びセーフ・モードのＯＳ起動に対応する。標準モードのＯＳ起動は、ユーザ（修理者も含む。）が、ＰＣの電源スイッチを”入”にするのみで、実施される。これに対して、セーフ・モードのＯＳ起動は、ＰＣの電源スイッチを”入”にすることの他に、ファンクション・スイッチＦ８を押す等、他の操作を要求される。したがって、所定のユーザ操作が行われたか否かを検知することにより、標準モード及びセーフ・モードのどちらのＯＳ起動を行うべきかを判断できる。セーフ・モードのシステム状態は、標準モードのシステム状態に対して、機能が制限されている。セーフ・モードのＯＳ起動及びシステム状態では、所定のトラブルにもかかわらず、ＰＣの作動を確保するために、必要最小限の機能のみが可能になっている。したがって、ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、セキュリティ・ハードウェア１１から読み出したセキュリティ・キー情報に基づいて判断する処理（以下、「セキュリティ・キー情報に基づくユーザ認証処理」と言う。）は第２の形式のＯＳ起動ではスキップされ、すなわち実施されず、また、第２の形式のＯＳ起動に基づくシステム状態としての第２のシステム状態では、高機能型のアプリケーションは実行不能になるか、低機能のみの通常のアプリケーションの実行は困難になっている。なお、セーフ・モードのシステム状態において、ＦＤ（フロッピ・ディスク）内のファイルをハード・ディスクへコピーする等の処理は可能であり、所定レベル以下の機能しかもたないプログラムの実行も可能である。

【００２７】

（Ｒ１）情報処理装置１０において第２のシステム状態を実施し、情報処理装置１０を第２の形式のＯＳ起動にする。図６のＯＳ起動形式選択手段１４では、第１及び第２の形式のＯＳの起動のどちらを実行するかを、所定ユーザ操作の検出手段２５による所定ユーザ操作の有無の検出に基づいて判断する。例えば、ＯＳがＷｉｎｄｏｗｓである場合、ＯＳ起動形式選択手段１４は、情報処理装置１０の電源スイッチが”入”にされた後、キーボードのＦ８キーを押し続けると言うユーザ操作があれば、第２の形式のＯＳ起動としてのセーフ・モード起動を実行し、該ユーザ操作がなければ、第１の形式のＯＳ起動としての標準モード起動を実行する。図７のＯＳ起動形式選択手段１４では、第１及び第２のシステム状態のいずれを実行するかを、ＯＳ３２をストアしている補助記憶装置３１がそれ用のドライブ（該ドライブは、システムへ接続状態になっていれば、内付け及び外付けのどちらでも可）に存在するか否かに基づいて判断する。一般のＰＣでは、ＦＤドライブやＣＤドライブにＯＳを読み取り自在のＦＤやＣＤ－ＲＯＭ等のメディアがあった場合、ハード・ディスクのＯＳより優先して交換可能メディアからＯＳを読み取って、それを起動するようになっている。セーフ・モードのためのＯＳ起動や補助記憶装置３１のＯＳ３２の起動では、機能が十分に制限された必要最小限機能の起動となるので、ＯＳ起動時のセキュリティ・キー情報に基づくユーザ認証は省略され、図３の窓は表示されることなく、ＯＳ起動が進み、情報処理装置１０は第２のシステム状態となる。

【００２８】

（Ｒ２）修理者は、情報処理装置が第２の形式のＯＳ起動になった後、所定のプログラム（該プログラムの名前を説明の便宜上、”ＣＳＳＲＴ（Ｃｌｉｅｎｔ Ｓｅｃｕｒｉｔｙ Ｓｏｆｔｗａｒｅ Ｒｅｐａｉｒ Ｔｏｏｌ）”と呼ぶことにする。）がストアされているＦＤをＦＤ用のドライブにセットし、プログラムＣＳＳＲＴを実行する。なお、ＦＤ用ドライブは、ＰＣに内蔵されていてもよいし、ＵＳＢ（Universal Serial Bus）ケーブルを介してＰＣ本体に分離自在に接続されるものであってもよい。プログラムＣＳＳＲＴは、無効化手段１５の機能を果たすＣＳＳＲＴ本体と無効解除手段１６の機能を果たす部分ＣＳＳＲＴ＿１

とを含み、部分ＣＳＳＲＴ＿１を、ＦＤから補助記憶装置としてのハード・ディスクにコピーするか、自ら作成してハード・ディスクにストアする。

【００２９】

（Ｒ３）プログラムＣＳＳＲＴの終了に伴い、情報処理装置１０は自動的に又は修理者の指示によりリスタート（Restart）する。注意すべきは、このリスタート時において、プログラムＣＳＳＲＴ＿１は、ハード・ディスクに残っているが、ＣＳＳＲＴ本体は情報処理装置１０のどこにも残らないことである。

【００３０】

（Ｒ４）修理者は、起動時に、所定ユーザ操作、例えばキーボードのＦ８キーを押し続けるというような所定ユーザ操作を省略する。ＯＳ起動形式選択手段１４は、所定のユーザ操作の有無を検出し、切替手段２６は、第１の形式のＯＳ起動の実施手段２３を作動させて、第１の形式のＯＳ起動を実行する。ＯＳ起動許容手段１２は、今回の第１の形式のＯＳ起動においては、無効化手段１５により作動を無効化されているので、修理者に対してＯＳ起動の許容のための図３のパスフレーズ、すなわちセキュリティ・チップのセキュリティ・キー情報に基づく認証としての認証用データの入力を求めない。こうして、情報処理装置１０は第１のシステム状態となる。なお、無効解除手段１６の機能を果たすＣＳＳＲＴ＿１は、無効解除手段１６の機能を果たすとともに、その機能終了後に自分自身としてのＣＳＳＲＴ＿１を削除する削除プログラムＣＳＳＲＴ＿１＿ＤＥＬ（図８の消去手段３７に相当するプログラム）を、ＣＳＳＲＴ＿１の存命中に作る。こうして、ハード・ディスク等の常備補助記憶装置に無効化処断１５及び無効解除手段１６が存在する期間は、極めて限定されたものとなる。なお、典型的には、ＣＳＳＲＴ＿１は、無効解除手段１６の機能実施後に、ＣＳＳを呼び出す機能も実施する。

【００３１】

（Ｒ５）修理者は、（Ｒ４）の後の第１のシステム状態において、セキュリティ・ハードウェア１１へのセキュリティ・キー情報の復元作業を行う。セキュリティ・キー情報復元手段１３は、所定の復元用データに基づいて復元したセキュリティ・キー情報をセキュリティ・ハードウェア１１へ書き込む。ＣＳＳでは、図

５を参照して前述したように、ハード・ディスク内の復元用データ・ファイルに基づいてセキュリティ・キー情報の復元が可能になっている。セキュリティ・キー情報復元手段１３は、例えば、図５のセキュリティ・キー情報復元用窓を介して入力された復元用データに基づいてセキュリティ・ハードウェア１１にセキュリティ・キー情報を復元する。

【００３２】

（Ｒ６）セキュリティ・キー情報復元手段１３によるセキュリティ・ハードウェア１１におけるセキュリティ・キー情報を復元したのに伴い、情報処理装置１０は、自動的に又は修理者の所定の指示を待ってリスタートする。ＣＳＳＲＴ＿１＿ＤＥＬは、このリスタート時に、又はＣＳＳＲＴ＿１の実行終了後でかつリスタート前の第１のシステム状態の期間に、作動して、ＣＳＳＲＴ＿１を削除するので、このリスタートでは、第１の形式のＯＳ起動にもかかわらず、無効化手段１５は作動せず、セキュリティ・キー情報に基づくユーザ認証が実施される。

【００３３】

消去手段３７の機能を実現するプログラムはハード・ディスクに残っていても、特に弊害はない。また、万一、無効解除手段１６に係るプログラムが常備補助記憶装置に残ったまま、修理者からユーザに情報処理装置１０が返却されたとしても、ユーザが自分のユーザ認証を要求されると言うことであり、不利なことは、使用しない余計なプログラムがハード・ディスクに残っていると言うことだけである。

【００３４】

図９は図１０のフローチャートに係るプログラムを実行するためのハードウェア構成図である。図１０のフローチャートに係る方法の各ステップは例えば図９のハードウェアを使用して実行される。システム・バス４３には、ＣＰＵ４４、主記憶装置４５及び入出力装置４６が接続される。後述の図１０のフローチャートに係る方法は、コード化されたプログラムとして実行可能となっている。入出力装置４６には、該プログラムをストアしてあるハード・ディスク等の補助記憶装置が含まれ、該プログラムは、ＣＰＵ４４において実行されるのに先立ち、主記憶装置４５にストアされる。ＣＰＵ４４は、主記憶装置４５の命令行を順次、

読み出して、該プログラムを実行する。

【００３５】

図１０は情報処理装置１０の制御方法のフローチャートである。該制御方法が適用される情報処理装置１０は、図１に記載されている通り、セキュリティ・ハードウェア１１、ＯＳ起動許容手段１２、セキュリティ・キー情報復元手段１３、及びＯＳ起動形式選択手段１４を有している。セキュリティ・ハードウェア１１は、セキュリティ・キー情報を読書き自在に格納する。ＯＳ起動許容手段１２は、ＯＳ起動の際にユーザ認証用の入力データが正当であるか否かを、セキュリティ・ハードウェア１１から読み出したセキュリティ・キー情報に基づいて判断し、該判断結果が”正”であればＯＳ起動を許容する。セキュリティ・キー情報復元手段１３は、所定の復元用データに基づいてセキュリティ・ハードウェア１１にセキュリティ・キー情報を復元する。ＯＳ起動形式選択手段１４は、セキュリティ・キー情報復元手段１３が作動可能となるシステム状態（以下、「第１のシステム状態」と言う。）を生成するＯＳ起動であってかつＯＳ起動許容手段１２が作動する第１の形式のＯＳ起動と、セキュリティ・キー情報復元手段１３が作動不可能である機能制限されたシステム状態（以下、「第２のシステム状態」と言う。）を生成するＯＳ起動であってかつＯＳ起動許容ステップが作動しない機能制限された第２の形式のＯＳ起動とのいずれかを選択して実施する。図１０のフローチャートにおいて、Ｓ５０では、無効化手段１５が、それが生成された以降の第１の形式のＯＳ起動におけるＯＳ起動許容手段１２の作動を無効にする。Ｓ５１では、ＯＳ起動許容手段１２が無効化手段により作動を無効化された第１の形式のＯＳ起動が少なくとも１回、実施された後、無効解除手段１６が、無効化手段１５による前記ＯＳ起動許容手段１２の作動の無効を解除する。

【００３６】

こうして、セキュリティ・ハードウェア１１を交換したときのセキュリティ・キー情報の復元では、修理者は、セキュリティ・ハードウェア１１のセキュリティ・キー情報に基づくＯＳ起動許容手段１２によるユーザ認証をスキップできる第２の形式のＯＳ起動により情報処理装置１０を第２のシステム状態にする。この後、プログラムの実行により、無効化手段１５が生成され、該無効化手段１５

は、次の第１の形式のＯＳ起動において、セキュリティ・ハードウェア１１のセキュリティ・キー情報に基づくＯＳ起動許容手段１２による認証を無効化させ、情報処理装置１０を、セキュリティ・ハードウェア１１におけるセキュリティ・キー情報の無存在にもかかわらず、第１のシステム状態にする。この第１のシステム状態の期間では、セキュリティ・ハードウェア１１におけるセキュリティ・キー情報の復元可能であり、セキュリティ・キー情報復元手段１３はセキュリティ・キー情報を復元する。無効解除手段１６は、無効化手段１５によるＯＳ起動許容手段１２の作動の無効を解除し、これにより、次の第１の形式のＯＳ起動からは再び、セキュリティ・ハードウェア１１のセキュリティ・キー情報に基づくＯＳ起動許容手段１２によるユーザ認証が実施される。

【００３７】

図１０のフローチャートに係る制御方法を適用される情報処理装置１０には、次の態様（ｃ１）～（ｃ６）の１個又は複数個を任意の組み合わせで付加したものを含む。

（ｃ１）ユーザ認証用の入力データは、第１の形式のＯＳ起動の際にユーザがキー入力するデータである。

（ｃ２）復元用データは、セキュリティ・ハードウェア１１内のセキュリティ・キー情報を生成した際に、セキュリティ・キー情報を復元自在のものとして生成されたものであり、補助記憶装置２１に保存されているものである。

（ｃ３）第１及び第２の形式のＯＳ起動は、同一の補助記憶装置２１内に保存されている同一のＯＳ２２に基づく起動であり、ＯＳ起動形式選択手段１４は、ＯＳ２２を起動しようとするときに、所定ユーザ操作の有無を検出して”無し”のときは第１の形式のＯＳ起動を、また、”有り”のときは第２の形式のＯＳ起動を、それぞれ選択して実施するものである。

【００３８】

（ｃ４）第１及び第２の形式のＯＳ起動は、それぞれ別の補助記憶装置２１，３１内に保存されているＯＳに基づく起動であり、ＯＳ起動形式選択手段１４は、第２のＯＳ３２を保存する補助記憶装置３１から第２のＯＳ３２を読み取り可能であるときは、第１の形式のＯＳ起動より第２の形式のＯＳ起動を優先して、選

択し、実施するものである。

（ｃ５）無効解除手段１６が無効化手段１５によるＯＳ起動許容手段１２の作動の無効を解除した後に、消去手段３７が無効解除手段１６を消去する消去ステップを有していること。

（ｃ６）上記（ｃ５）のステップに加えて、無効解除手段１６が消去手段３７を生成するステップを有していること。

【００３９】

図１１は図１０のフローチャートに上記（ｃ５）及び（ｃ６）に対応するステップを付加したフローチャートである。Ｓ５３は、Ｓ５１とＳ５４との間に配置されてもよい。Ｓ５３では、無効解除手段１６が消滅手段３７を生成する。Ｓ５４では、消滅手段３７が無効解除手段１６を消去する。

【００４０】

【発明の効果】

本発明によれば、ＯＳ起動時にセキュリティ・ハードウェアのセキュリティ・キー情報に基づいてユーザ認証を行う情報処理装置において、故障修理等のためにセキュリティ・ハードウェアを交換したときに、新規なセキュリティ・ハードウェアに旧セキュリティ・ハードウェアのセキュリティ・キー情報を復元することができる。

【図面の簡単な説明】

【図１】

情報処理装置のブロック図である。

【図２】

携帯型ＰＣ及びデスク・トップ型ＰＣを示す図である。

【図３】

セキュリティ・ハードウェアのセキュリティ・キー情報に基づくユーザ認証用の窓を例示した図である。

【図４】

ＯＳに基づくユーザ認証用窓の例示した図である。

【図５】

セキュリティ・ハードウェアにおけるセキュリティ・キー情報を復元する際の作業窓を例示した図である。

【図６】

所定態様のＯＳ起動形式選択手段を装備する情報処理装置のブロック図である。

【図７】

別の所定態様のＯＳ起動形式選択手段を装備する情報処理装置のブロック図である。

【図８】

消去手段が付加された情報処理装置のブロック図である。

【図９】

図１０のフローチャートに係るプログラムを実行するためのハードウェア構成図である。

【図１０】

情報処理装置の制御方法のフローチャートである。

【図１１】

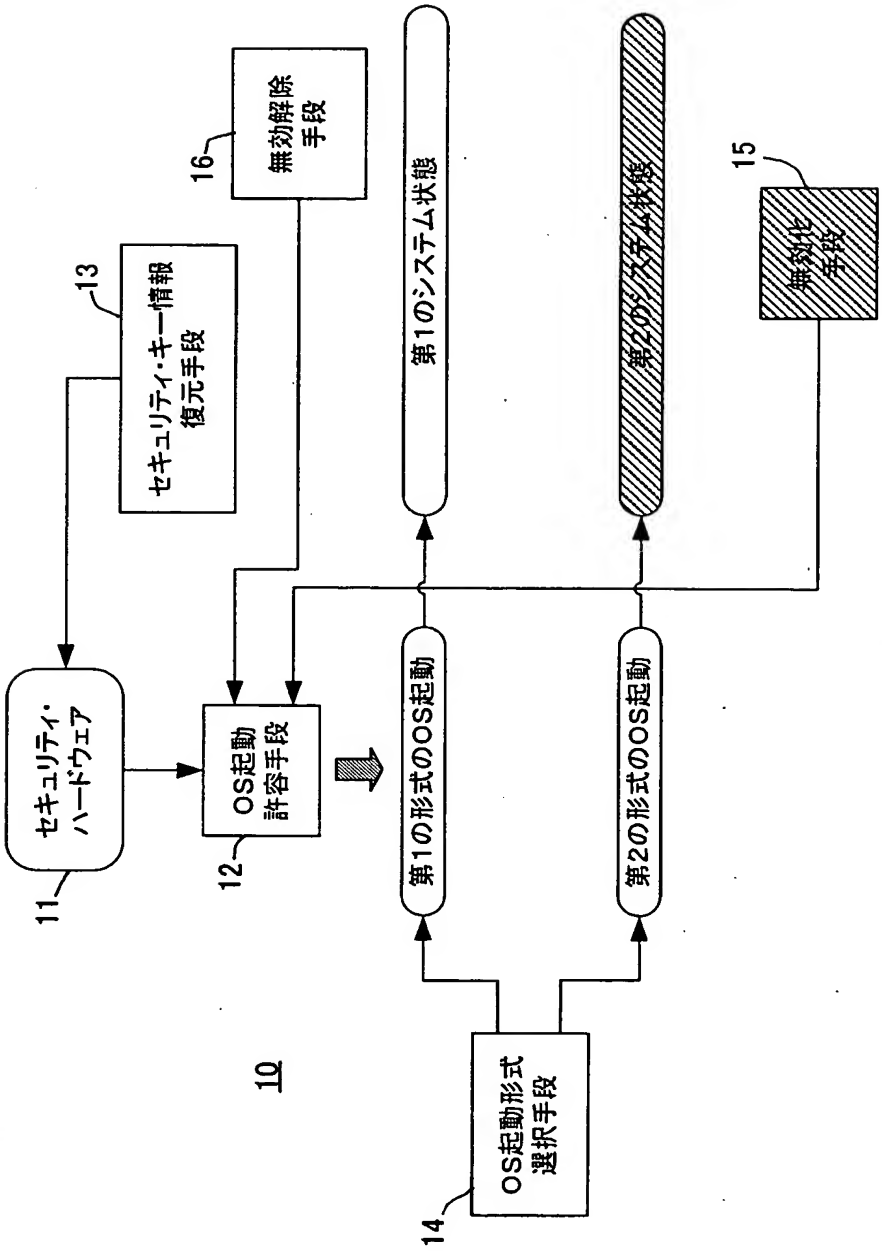
図１０にさらに所定のステップを付加したフローチャートである。

【符号の説明】

１０：情報処理装置、１１：セキュリティ・ハードウェア、１２：ＯＳ起動許容手段、１３：セキュリティ・キー情報復元手段、１４：ＯＳ起動形式選択手段、１５：無効化手段、１６：無効解除手段、２１：補助記憶装置、２２：ＯＳ、２３：第１の形式のＯＳ起動の実施手段、２４：第２の形式のＯＳ起動の実施手段、２５：所定ユーザ操作の検出手段、２６：切替手段、３４：メディア検出手段、。

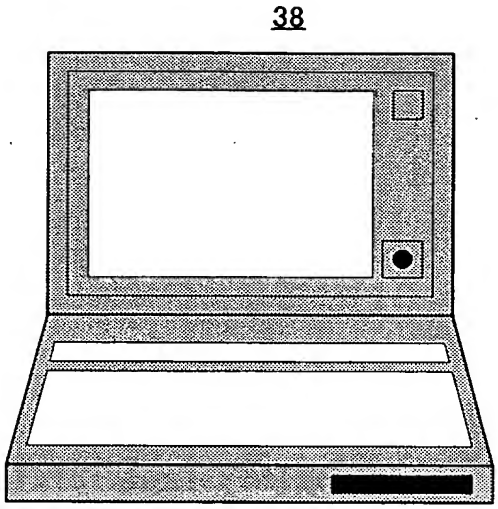
【書類名】　図面

【図１】

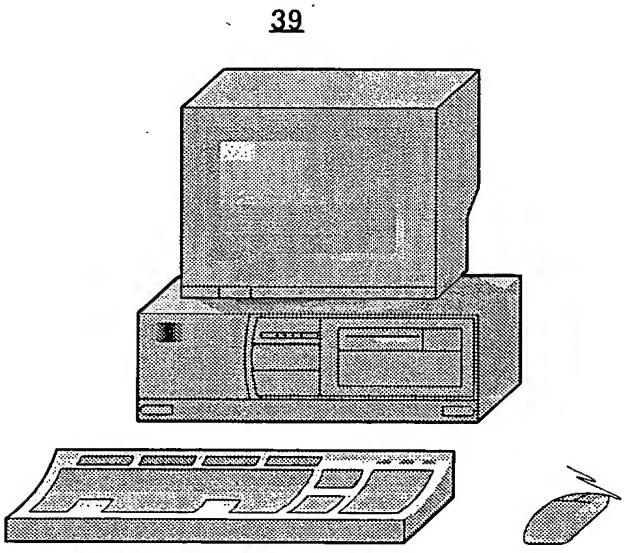

10
11
セキュリティ・ハードウェア
12
OS起動許容手段
13
セキュリティ・キー情報復元手段
14
OS起動形式選択手段
15
無効化手段
16
無効解除手段
第1のシステム状態
第2のシステム状態
第1の形式のOS起動
第2の形式のOS起動

【図２】

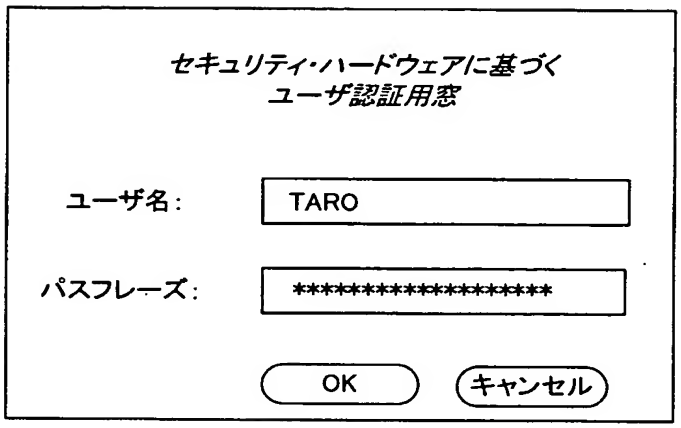
(a)



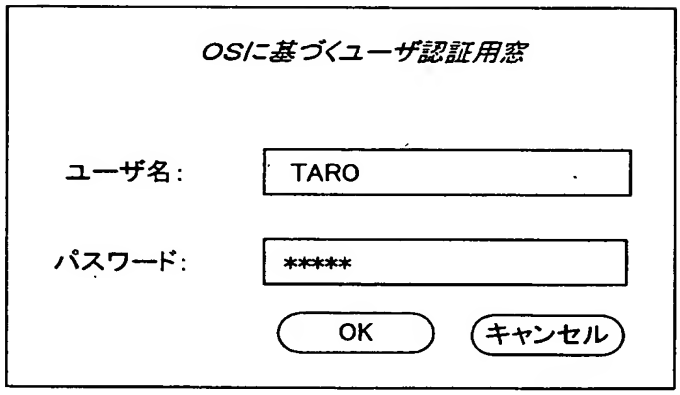
(b)



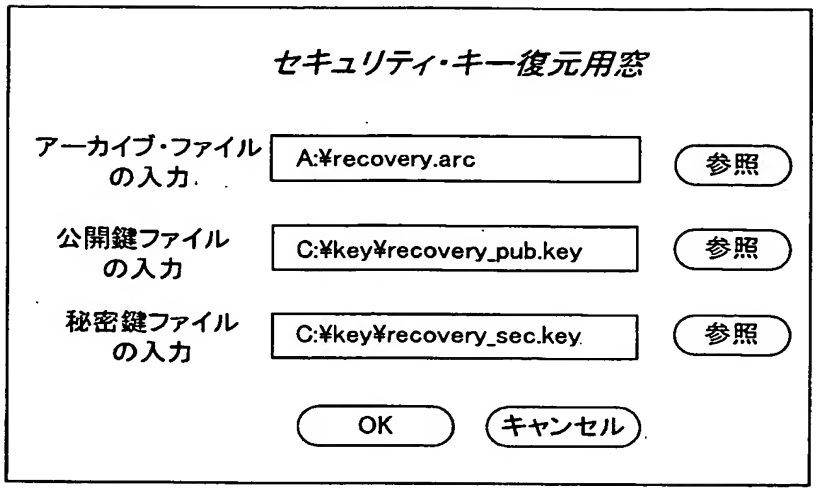
【図３】


セキュリティ・ハードウェアに基づく
ユーザ認証用窓
ユーザ名：
TARO
パスフレーズ：
****
OK
キャンセル

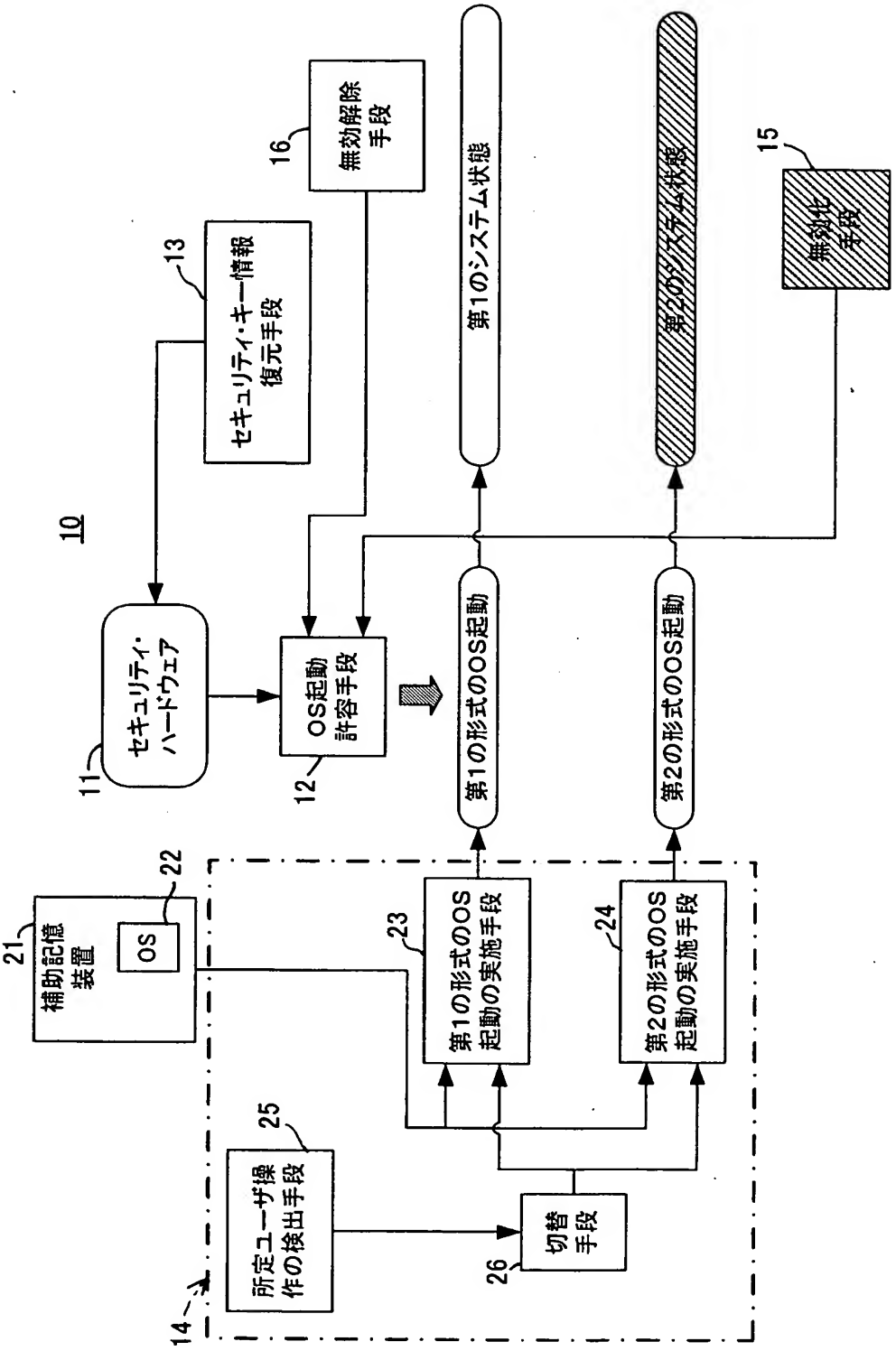
【図４】


OSに基づくユーザ認証用窓
ユーザ名：
TARO
パスワード：
*****
OK
キャンセル

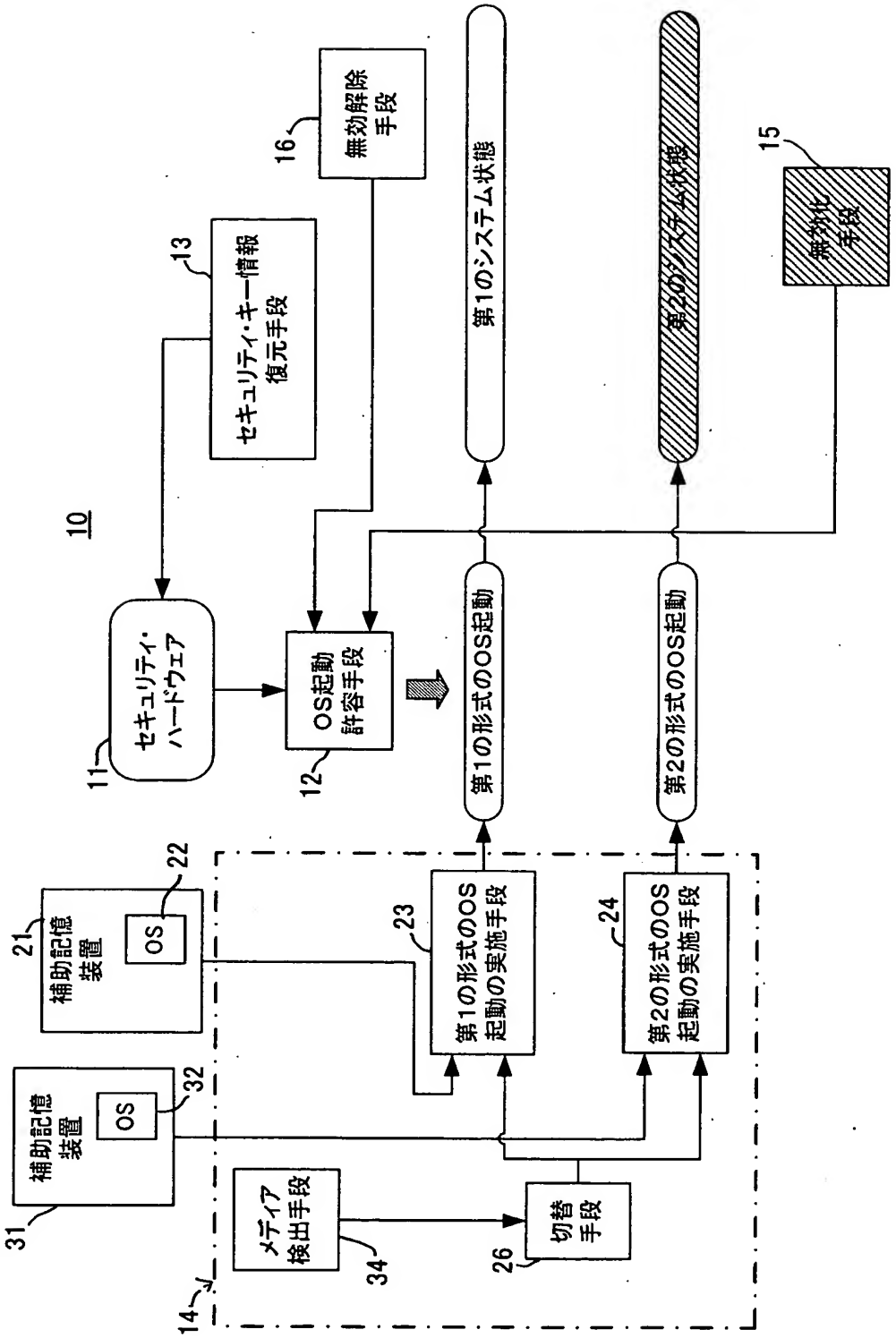
【図５】


セキュリティ・キー復元用窓
アーカイブ・ファイルの入力
A:¥recovery.arc
参照
公開鍵ファイルの入力
C:¥key¥recovery_pub.key
参照
秘密鍵ファイルの入力
C:¥key¥recovery_sec.key
参照
OK
キャンセル

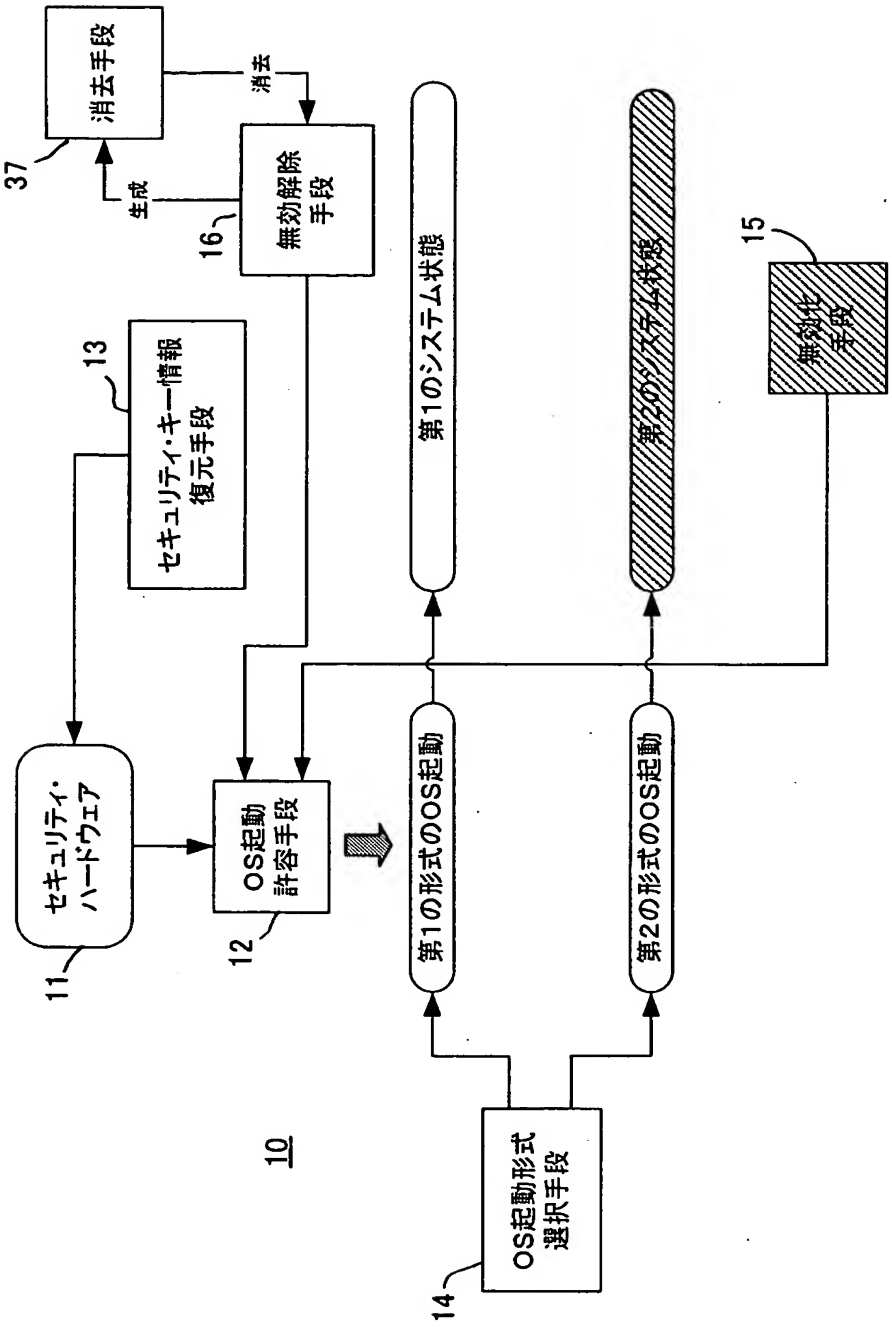
【図６】


10
セキュリティ・ハードウェア
11
OS起動許容手段
12
セキュリティ・キー情報復元手段
13
無効解除手段
16
無効化手段
15
第1のシステム状態
第2のシステム状態
第1の形式のOS起動
第2の形式のOS起動
補助記憶装置
21
OS
22
第1の形式のOS起動の実施手段
23
第2の形式のOS起動の実施手段
24
所定ユーザ操作の検出手段
25
切替手段
26
14

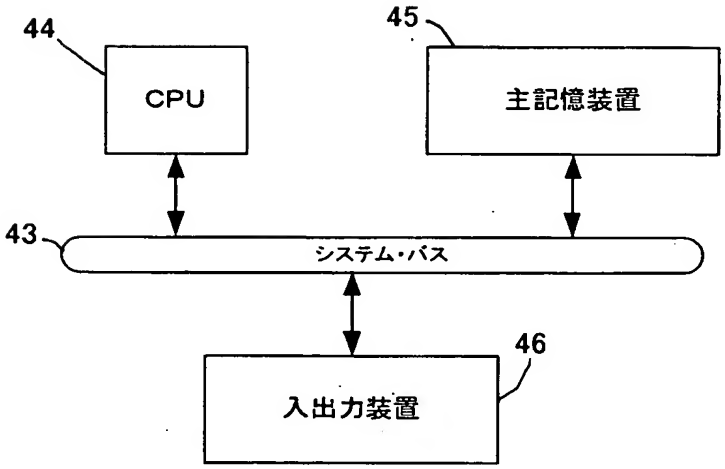
【図７】


10
セキュリティ・ハードウェア
11
OS起動許容手段
12
セキュリティ・キー情報復元手段
13
無効解除手段
16
無効化手段
15
第1のシステム状態
第2のシステム状態
第1の形式のOS起動
第2の形式のOS起動
補助記憶装置
OS
21
22
補助記憶装置
OS
31
32
第1の形式のOS起動の実施手段
23
第2の形式のOS起動の実施手段
24
メディア検出手段
34
切替手段
26
14

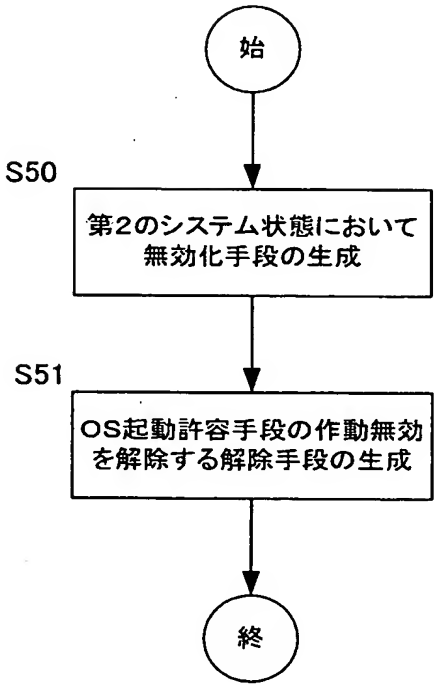
【図８】


消去手段
37
消去
生成
無効解除手段
16
セキュリティ・キー情報復元手段
13
セキュリティ・ハードウェア
11
OS起動許容手段
12
第1のシステム状態
第2のシステム状態
15
無効化手段
第1の形式のOS起動
第2の形式のOS起動
OS起動形式選択手段
14
10

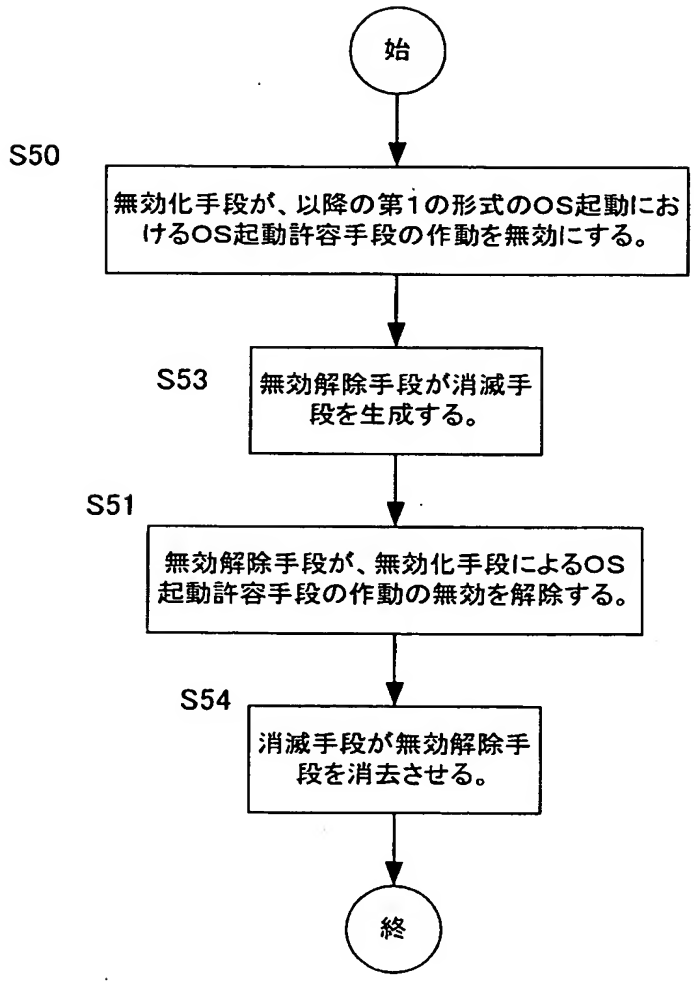
【図９】


44
CPU
45
主記憶装置
43
システム・バス
46
入出力装置

【図１０】


始
S50
第2のシステム状態において
無効化手段の生成
S51
OS起動許容手段の作動無効
を解除する解除手段の生成
終

【図１１】


始
S50
無効化手段が、以降の第1の形式のOS起動におけるOS起動許容手段の作動を無効にする。
S53
無効解除手段が消滅手段を生成する。
S51
無効解除手段が、無効化手段によるOS起動許容手段の作動の無効を解除する。
S54
消滅手段が無効解除手段を消去させる。
終

【書類名】　　要約書

【要約】

【課題】　ＯＳ起動時にセキュリティ・ハードウェア１１のセキュリティ・キー情報に基づいてユーザ認証を行う情報処理装置１０において、故障修理により交換した後のセキュリティ・ハードウェア１１に交換前のセキュリティ・キー情報を復元する。

【解決手段】　無効化手段１５は、セーフ・モード等の機能制限された第２の形式のＯＳ起動により生じる第２のシステム状態において、生成される。第１の形式のＯＳ起動では、通常は、セキュリティ・ハードウェア１１のセキュリティ・キー情報に基づくユーザ認証が実施されるが、無効化手段１５はこれを無効化する。これにより、ユーザ認証を受けずに、情報処理装置１０を第１のシステム状態にでき、セキュリティ・キー情報の復元が可能になる。無効解除手段１６はユーザ認証の無効化を解除し、セキュリティ・キー情報の復元後では、第１の形式のＯＳ起動時のユーザ認証が復活する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－０２９８１３
受付番号	５０３００１９２９７０
書類名	特許願
担当官	塩野　実　　２１５１
作成日	平成１５年　２月　７日

＜認定情報・付加情報＞

【提出日】　平成15年 2月 6日

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100108501

【住所又は居所】　神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社　知的所有権

【氏名又は名称】　上野　剛史

【復代理人】　申請人

【識別番号】　100085408

【住所又は居所】　東京都中央区日本橋２丁目１番１号　櫻正宗ビル９階

【氏名又は名称】　山崎　隆

次頁無

特願２００３－０２９８１３

出　願　人　履　歴　情　報

識別番号　　［３９０００９５３１］

１．変更年月日　　２０００年　５月１６日
［変更理由］　　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション

２．変更年月日　　２００２年　６月　３日
［変更理由］　　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション